

REMARKS

This is a response to Office Action dated October 19, 2004. Claims 1-11, 13, 14 and 16-19 are pending in the present application. Claims 1, 2, 3, 4, 7, 8, 9, 10, 11, 13 and 14 have been amended, claims 12 and 15 have been amended, and claims 16-19 have been added. The new claims do not introduce new matter and are entirely supported by the specification. In this Office Action, the Examiner objected to the abstract, claim 8 and claim 14. Next, the Examiner rejected claims 2 and 4-6 as being anticipated by U.S. Patent Application No. 2001/0044905 to Novak et al. (Novak). The Examiner rejected claims 1 and 15 as being obvious over the Novak reference in view of U.S. Patent No. 5,548,649 to Jacobson (the '649 patent). The Examiner also rejected claims 3, 7-9 and 12-13 as being obvious over the Novak reference in view of U.S. Patent Application No. 2002/0010866 to McCullough et al. (McCullough). The Examiner also rejected claims 10 and 11 as being obvious over the Novak reference in view of U.S. Patent Application 2002/0019933 to Friedman et al. (Friedman). Individual issues raised by the Examiner are addressed next in the order in which they appear in the Office Action.

Specification

In paragraph 1 of the Office Action, abstract of the disclosure was objected to because it exceeded 150 words in length. In response, applicants submit herewith a replacement abstract that is believed to conform with the MPEP § 608.01(b) requirements.

Claim Objections

In paragraph 2 of the Office Action, claim 8 was objected to because of an informality. Claim 8 has been amended to correct the informality. Claim 14 has been amended to more particularly point out and distinctly claim the subject matter which the Applicants regard as the invention. As such, the 112, second paragraph, rejection of claim 14 should be withdrawn.

Claim Rejections Under 35 U.S.C. § 102(e)

In paragraphs 5-6 of the Office Action, claims 2 and 4-6 were rejected under 35 U.S.C. 102(e) as being anticipated by the Novak reference. In addition, in paragraph 7 of the Office Action, claim 14 was rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application No. 6,084,969 to Wright et al. (the '969 patent).

Applicant amended independent claim 2. Applicant respectfully submits that amended claim 2 is patentable over the Novak reference. In particular, this claim is patentable at least because the cited reference fails to teach all of the elements of this claim.

In particular, the Novak reference is directed to a system and method for providing secure data transfer between network nodes by way of a three layer hierarchical structure (*See, e.g., Abstract*). The three layer hierarchical structure is constructed using a secure system kernel that manages secure servers, secure servers that provide security services to clients and secure clients that transmit secure messages to secure servers (*See, e.g., paragraph [0018] – [0021]*). Security is achieved by transferring data from a secure client A1 to a secure server A using various ciphering languages available on secure server A (*See, e.g., FIG 3 and paragraph 0017*). Novak also teaches that a “network user” becomes a secure client by registering with at least one secure server (*See, e.g., paragraph [0054]*). For a secure client A1 to transmit an encrypted message to secure client A3 over a public network, secure client A1 encrypts the message using a ciphering language that is associated with secure client A3 and is received from secure server A. Secure client A3 uses the same ciphering language to decrypt the message sent by the secure client A1 (*See e.g., paragraph [0069] and FIG 3*).

The system of the present application is directed to a method and system for secured transport and storage of data on a network.

Claim 2 is directed toward “a method for transmitting packets in a secure format from a first node to a second node.” Claim 2 has been amended to recite that, *inter alia*, “receiving secure packets in a first secure relay or a second secure relay from the first node, wherein said secure packets contain retrieval information based on information provided by the first node,” “determining if a retrieval condition has been indicated by identifying said secure packets that contain the same retrieval information based on information provided by the second node,” and “forwarding all secure packets associated with the retrieval condition to the second node if the retrieval condition has been indicated, wherein said second node may be the first node.” No new matter has been added.

Unlike the method of claim 2, the Novak reference does not teach “receiving secure packets in a first secure relay or a second secure relay from the first node, wherein said secure packets contain retrieval information based on information provided by the first node,” as recited in claim 2. Rather the secure client A1 in the Novak reference transmits all secure messages to a secure server A using the secure server A’s transmission ciphering set

(paragraph [0069] and FIG. 3). As such, all packets are transmitted directly to secure sever A and no other server. Thus Novak does not transmit packets to a "second secure relay, wherein the second secure relay is a different secure relay from the first secure relay" as recited in claim 2. Further, the encrypted message sent in the Novak reference does not "contain retrieval information based on information provided by the first node," as required by claim 2. Instead, the encrypted message in the Novak reference is encrypted based on a ciphering language stored in the secure server A (paragraph [0057]).

Moreover unlike the method of claim 2, Novak does not teach "determining if a retrieval condition has been indicated by identifying said secure packets that contain the same retrieval information based on information provided by the second node" as required in claim 2. As demonstrated in FIG 3 of the Novak reference, the message is sent directly to receiving client A3 without regard to a retrieval condition. Upon reaching client A3, Novak teaches to "decrypt the message using a ciphering set." (see paragraph [0069]). In fact, the Novak reference would have no need to "determine if a retrieval condition has been indicated by identifying said secure packet that contain the same retrieval information" as required in claim 2, since the Novak reference teaches encrypting the message based on a ciphering set in a secure server A. Moreover, the Novak reference cannot identify "secure packets that contain the same retrieval information," as required by claim 2. As such, the Novak reference cannot determine "if a retrieval condition has been indicated based on information provided by the second node" as required by claim 2.

Moreover unlike the present invention, the Novak reference does not teach "forwarding all secure packets associated with the retrieval condition to the second node if the retrieval condition has been indicated, wherein said second node may be the first node" as required in claim 2. The Novak fails to teach or suggest this limitation. Public Server 2, 4 and 3 merely transmit the encrypted message to client A3 and do not "forward all secure packets associated with the retrieval condition," as required in claim 2. Moreover, the Novak reference has no need to determine whether or not a "retrieval condition" has or has not been indicated, since the Novak reference teaches forwarding the entire encrypted message to client A3 via Public Servers.

Accordingly for the above stated reasons, Applicants submit that the Novak reference does not teach all of the elements of claim 2. As such, the 102(e) rejection is improper and this rejection should be withdrawn.

Claims 3, 4, 5, 6, 7, 13 and 14 and new claims 18 and 19 depend from claim 2 either directly or indirectly. Each of these claims is considered to be patentable over the applied art. Each includes limitations of the claims from which it depends and recites subject matter not taught or suggested by the applied art in the claimed combination.

In addition, claim 4 adds the additional limitation of, *inter alia*, "receiving a retrieval packet from the second node in the first and second secure relays that indicates the retrieval condition for secure packets, wherein said retrieval packet contains a flag that instructs said first and second secure relays to identify secure packets that contain the same retrieval information." The Novak reference fails to teach or suggest this limitation. Unlike the method of claim 4, Client A3 merely receives encrypted messages from the Public Network Server 3 (paragraph [0069]). As such, the 102(e) rejection is improper and this rejection should be withdrawn.

In addition, new claim 19 adds the additional limitation of, *inter alia*, "successively forwarding multiple identical retrieval packets to the first and second secure relays." The Novak reference fails to teach or suggest this limitation. Unlike the method of claim 19, Client A3 merely receives encrypted messages from the Public Network Server 3 (paragraph [0069]).

Further, claim 14 is considered to be patentable over the '969 patent. Claim 14 includes the limitations of claim 2 and recites subject matter not taught or suggested by the applied art. At least for the reasons explained above, the '969 patent or the Novak reference fail to teach the limitations in claim 14.

For at least the reasons given above, these claims are thus not anticipated by the Novak reference or the '969 patent. Accordingly, independent claim 2 as well as claims 3, 4, 5, 6, 7, 13, 14 and claims 18-19 dependent thereon, are patentable over the applied art.

Claim Rejections Under 35 U.S.C. § 103(a)

In paragraph 9 of the Office Action, claims 1 and 15 were rejected under 35 U.S.C. 103(a) as being obvious over the Novak reference in view of the '649 patent. Applicant amends independent claim 1 and cancels independent claim 15. The Novak reference and the '649 patent fail to disclose all limitations of independent claim 1.

Claim 1 is directed toward "secure transport system for transporting secure packets from a first node to a second node." Claim 1 has been amended to recite that, *inter alia*, "a first node that creates secure packets, wherein each secure packet contains identical retrieval

information," "multiple secure relays that receive secure packets and non secure packets from multiple nodes or other secure relays, wherein said multiple secure relays are capable of identifying retrieval information in each secure packet ... and wherein each of said multiple secure relays forwards secure packets to another of said multiple secure relays when the retrieval condition has not been indicated," and "a second node that creates a retrieval condition related to said retrieval information in said multiple secure packets and receives the secure packets, wherein said first or second nodes are not associated with said multiple secure relays." No new matter has been added.

The Office Action admits that the Novak reference does not teach a first secure relay that receives non secure packets, but alleges that the Novak reference, combined with the network security bridge of the '649 patent, would render independent claim 1 obvious. The combination fails to teach the claimed invention, since neither reference recites all limitations of independent claim 1.

Unlike the system of claim 1, the Novak reference does not teach "a first node that creates secure packets, wherein each secure packet contains identical retrieval information," as recited in claim 1. Rather the secure client A1 in Novak encrypts the secure message using a private ciphering language that belongs to the pair of communicating secure elements (paragraph [0075] and FIG 7). As such, all messages are encrypted and do not "contain identical retrieval information" as recited in claim 1.

Moreover unlike the system of claim 1, Novak does not teach "multiple secure relays that receive secure packets and non secure packets from multiple nodes or other secure relays, wherein said multiple secure relays are capable of identifying retrieval information in each secure packet ... and wherein each of said multiple secure relays forwards secure packets to another of said multiple secure relays when the retrieval condition has not been indicated" as recited in claim 1. As demonstrated in FIG 3 of the Novak reference, encrypted messages are sent to receiving client A3 without regard to retrieval information. To determine the proper recipient of the encrypted message, the Novak reference teaches decrypting the security header at an authorized secure server so as to determine the destination client (paragraph [0061]). Unauthorized secure servers are unable to decrypt the security header and merely forward the encrypted message to another secure server (paragraph [0063]). As such, Novak would have no need to "identify retrieval information in each secure packet" as required in claim 1 since the original message was previously encrypted using a private ciphering key set (paragraph [0075]). Moreover, the Novak

reference would have no need to "forward secure packets to another of said multiple secure relays when the retrieval condition has not been indicated" as required in claim 1 since in all instances the Novak reference merely forwards the encrypted message to a Public Network Server 3 without regard to a retrieval condition.

Moreover, unlike the system of claim 1, the Novak reference does not teach "a second node that creates a retrieval condition related to said retrieval information in said multiple secure packets and receives the secure packets, wherein said first or second nodes are not associated with said multiple secure relays," as recited in claim 1. Rather secure clients A1 and A3 as well as Server A are all related. In fact, Server A contains the encryption and decryption ciphering sets related to each client (paragraph [0069]). As such, the Novak reference could not have nodes that are not associated with multiple secure relays since in order for client A3 to decrypt a message sent from client A1, client A1 must utilize a ciphering set in common to both clients that is stored on Server A.

The Novak reference simply does not disclose or even suggest the above stated limitations. Similarly, nor does the '649 patent disclose this functionality. Accordingly, independent claim 1, as well as the claim dependent thereon, are patentable over the Novak reference and the '649 patent.

Claims 16 and 17 directly depends from claim 1. These claims are considered to be patentable over the applied art. Claims 16 and 17 include limitations of claim 1 and recite subject matter not taught or suggested by the applied art in the claimed combination.

For at least the reasons given above, these claims are thus not anticipated by the Novak reference or the '649 patent. Accordingly, independent claim 1 as well as claims 16 and 17 dependent thereon, are patentable over the applied art.

In paragraph 10 of the Office Action, claims 3, 7-9 and 12-13 were rejected under 35 U.S.C. 103(a) as being obvious over the Novak reference in view of the McCullough reference. Applicant amend independent claim 8 and cancel claim 12. The Novak reference and the McCullough reference fail to disclose all limitations of independent claim 8.

Claims 3, 7 and 13 depend from claim 2 either directly or indirectly. Each of these claims is considered to be patentable over the applied art. Each includes limitations of the claims from which it depends and recites subject matter not taught or suggested by the applied art in the claimed combination.

In addition, claim 3 adds the additional limitation of, *inter alia*, "providing a unique identifying flag from the second node to the first and second secure relays, wherein said unique identifying flag identifies secure packets that contain the same retrieval information. The Novak reference fails to teach or suggest this limitation. Unlike the method of claim 3, Client A3 merely receives encrypted messages from the Public Network Server 3 (paragraph [0069]).

For the reasons explained above, the Novak reference simply does not disclose or even suggest the above stated limitations. Similarly, nor does the McCullough reference disclose this functionality. Accordingly, claims 3, 7 and 13 are patentable over the Novak reference and the McCullough reference.

Claim 8 is directed toward "a method for maintain a secure distributed storage system by initiating a transmission of a message from a first node to a second node in a secure manner." Claim 8 has been amended to recite that, *inter alia*, "creating a set of secure packets associated with the message, wherein each secure packet contains an identical first retrieval key, wherein the first retrieval key is created by the first node," "forwarding the set of secure packets to multiple secure relays from the first node," and "forwarding the set of secure packets to among secure relays so long as a second retrieval key associated with the first retrieval key is not received in the said multiple secure relays, wherein said second retrieval key is created by the first or second node."

Unlike the method of claim 8, the Novak reference cannot "maintain a secure distributed storage system," as recited in claim 8. Rather the Novak reference merely teaches transmitting encrypted messages from client A1 to client A3. Moreover, unlike the method of claim 8, the Novak reference fails to teach or suggest "secure packets contain[ing] identical first retrieval key" or a "second retrieval key ... created by the first or second node," as recited in claim 8. Rather the encrypted message is transferred to client A3 from client A1 (paragraph [0069]). As such, the Novak reference has no need to create a "first retrieval key" or a "second retrieval key" as required in claim 8 since client A1 relies on secure server A to encrypt the message and client A3 relies on secure server A to decrypt the message.

Applicant submits that the McCullough reference does not cure the deficiencies inherent in the Novak reference. Thus, Applicant submits that the subject matter in claim 8 is patentably distinguishable from the prior art cited by the Examiner. Accordingly, independent claim 8, as well as the claim dependent thereon, are patentable over the Novak reference and the McCullough reference.

Claim 9 directly depends from claim 8. This claim is considered to be patentable over the applied art. Claim 9 includes limitations of claim 8 and recites subject matter not taught or suggested by the applied art in the claimed combination.

In addition, claim 9 adds the additional limitation of, *inter alia*, "creating a second retrieval key in a second node, wherein said second retrieval key is associated with destination information for the set of secure packets and information for identification of said first retrieval key." The Novak reference fails to teach or suggest this limitation. Unlike the method of claim 9, Client A3 merely receives encrypted messages from the Public Network Server 3 (paragraph [0069]).

For the reasons explained above, the Novak reference simply does not disclose or even suggest the above stated limitations. Similarly, nor does the '649 patent disclose this functionality. Accordingly, claim 9 is patentable over the Novak reference and the McCullough reference.

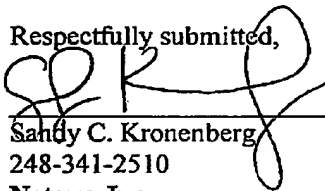
In paragraph 10 of the Office Action, claims 10 and 11 were rejected under 35 U.S.C. 103(a) as being obvious over the Novak reference in view of the Friedman reference. Claims 10 and 11 depend from claim 8. As such, claims 10 and 11 are considered to be patentable over the applied art. Claims 10 and 11 include limitations of claim 8 and recite subject matter not taught or suggested by the applied art in the claimed combination. For the reasons explained above, the Novak reference simply does not disclose or even suggest the above stated limitations. Similarly, nor does the Friedman disclose this functionality. Accordingly, claims 10 and 11 are patentable over the Novak reference and the Friedman reference.

Conclusion

On the basis of the above it is respectfully submitted that claims 1-11, 13, 14 and 16-19 of the present application are in a condition for allowance. A prompt action by the Examiner to this effect is respectfully requested. Should the Examiner have any questions or comments concerning this submission, or any aspect of the application, the Examiner is invited to call the undersigned at the phone number listed below.

Date: April 11, 2005

Respectfully submitted,


Sandy C. Kronenberg
248-341-2510
Netarx, Inc.